SAND2017-11197R

Evaluation of Roadmap to Achieve Energy Delivery Systems Cybersecurity

Adrian Chavez
Sandia National Laboratories

1. Overview

The Department of Energy/Office of Electricity Delivery and Energy Reliability (DOE/OE) Cybersecurity for Energy Delivery Systems (CEDS) program is currently evaluating the Roadmap to Achieve Energy Delivery Systems Cybersecurity document that sets a vision and outlines a set of milestones. The milestones are divided into five strategic focus areas that include: 1. Build a Culture of Security; 2. Assess and Monitor Risk; 3. Develop and Implement New Protective Measures to Reduce Risk; 4. Manage Incidents; and 5. Sustain Security Improvements. The most current version of the roadmap was last updated in September of 2016.

Sandia National Laboratories (SNL) has been tasked with revisiting the roadmap to update the current state of energy delivery systems cybersecurity protections. SNL is currently working with previous and current partners to provide feedback on which of the roadmap milestones have been met and to identify any preexisting or new gaps that are not addressed by the roadmap. The specific focus areas SNL was asked to evaluate are: 1. Develop and Implement New Protective Measures to Reduce Risk and 2. Sustain Security Improvements.

SNL has formed an Industry Advisory Board (IAB) to assist in answering these questions. The IAB consists of previous partners on past CEDS funded efforts as well as new collaborators that have unique insights into the current state of cybersecurity within energy delivery systems. The IAB includes asset owners, utilities and vendors of control systems. SNL will continue to maintain regular communications with the IAB to provide various perspectives on potential future updates to further improve the breadth of cybersecurity coverage of the roadmap.

2. IAB Participants

The current IAB that we have reached out to consists of several past and current partners of SNL. Each of the partners were contacted to provide input on how best the roadmap can be revised to remove milestones that have been adequately addressed and to identify any existing gaps within the roadmap. We also asked for

U.S. DEPARTMENT OF ENERGY

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology and Engineering Solutions of Sandia LLC, a wholly owned subsidiary of Honeywell International Inc. for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

Sandia National Laboratories

the IAB to provide evidence of existing tools that address milestones that are being met. The information provided in this report were developed based on responses from the following IAB members:

1. Schweitzer Engineering Laboratories (SEL)
2. Ft. Belvoir Night Vision and Electronics Sensors Directive (NVESD)
3. An Oil and Natural Gas (ONG) Company
4. Tennessee Valley Authority (TVA)
5. SolarCity
6. Dominion Virginia Power (DVP)
7. The UNITE working group composed of 20+ asset owners and vendors

Responses were received by each of the IAB members and are summarized in the sections that follow. Each of the IAB members initially were provided with an Excel spreadsheets for each of the two strategic focus areas of SNL within the roadmap. In each spreadsheet, each of the milestones of the roadmap were enumerating in the first column and then an additional column was added for the IAB to complete regarding whether or not the specific milestones have or have not been met. A third column was added to allow the IAB member to provide any additional comments or questions. The results of the IAB responses are shown below.

3. IAB 2016 Milestones Addressed

The two strategic areas covered in this report are “Develop and Implement New Protective Measures to Reduce Risk” and “Sustain Security Improvements”. The first strategic area includes new technologies to harden energy delivery systems and make them more resilient to cyber incident while not degrading operational services. The second strategic area focuses on collaboration amongst national laboratories, academia, vendors, and asset owners to ensure that new technologies do not compromise the security of the overall energy delivery system. The following tables describe the progress thus far in meeting the milestones set within the roadmap. The feedback received for this table are in response to the roadmap document that was published in September 2011.

3.1 Develop and Implement New Protective Measures to Reduce Risk

	Milestones	Available Technologies/Solutions
Near-Term Goals	Capabilities to evaluate the robustness and survivability of new platforms, systems, networks, architectures,	• Monitor alerts from other organizations and vendors. Use a threat intelligence feed to collect this

	policies, and other system changes commercially available	information. • Nessus • Spirent
Mid-Term Goals	Scalable Access Control for all energy delivery system devices available	• Use Work Groups and Active Directory domain controllers. • Vendors of PCN applications need to begin to provide access control capabilities within applications themselves. Need to go beyond the infrastructure to application authorization. • Project Alliance SEL-3800/3801
	Next-generation, interoperable, and upgradeable solutions for secure serial and routable communications between devices at all levels of energy delivery system networks implemented	• Promoting the use of encryption on traffic sent via modem to cloud providers that assist in data collection for analysis and provide control capability. • There are published internal standards for using machine to machine cellular based networks as the first mile and field portions of PCNs (includes encryption requirements, firewall barriers at perimeters, contract language, etc.). Would like to see adoption of these

		standards as lifecycles of PCNs allow. • Project Lemnos SEL-3620/3622 • Cisco IE 3000 series switch combined with OSIsoft
Long-Term Goals	Self-configuring energy delivery system network architectures widely available	• SEL-2740 • Passive optic network solution - backbone solution • Acropolis can accept energy data and protect it as well
	Capabilities that enable security solutions to continue operation during a cyber attack available as upgrades and built-in to new security solutions	• Artificial Diversity and Defense Security (ADDSec) SEL-2740
	Next-generation, interoperable, and upgradeable solutions for secure wireless communications between devices at all levels of energy delivery system networks implemented	• Today SDNs (Software Defined Networks) are available that don't rotate endpoint IDs but do spread traffic across multiple paths and constantly rotate the paths. This obscures the true network. (Vendor example: Dispersive Technologies). This technique can be used with any network having right characteristics. Would want to adopt something like this in

		the future. - Mesh networks - zigbee license to government. Send data to random location. - JF12 certification in progress for SEL-3031
Overall Goal	Next-generation energy delivery system architectures provide "defense in depth" and employ components that are interoperable, and able to continue operating in a degraded condition during a cyber incident	- Continue to move towards overall goal listed of "defense-in-depth." - Pursue an autonomous environment. - Pursue resilience to continue operations during cyber attack. - Moving toward better integration/interoperability among vendors/devices.

3.2 Sustain Security Improvements

	Milestones	Available Technologies/Solutions
Near-Term Goals	Cyber threats, vulnerability, mitigation strategies, and incidents timely shared among appropriate sector stakeholders	- Grass Marlin (NSA) - Snort - CSET - ONG-ISAC - Oil & Natural Gas Information Sharing & Analysis Center - OGCSN - Oil & Gas Cybersecurity Network - OGBC - Oil & Gas Benchmarking

		Consortium • API-ITSS - API IT Security Subcommittee • E ISAC - Energy ISAC (Run by NERC) • Dynamic Application Scanning • Infrastructure Scanning • Perform Penetration Testing through various vendors • Threat Intelligence Feeds from vendor • Threat Intelligence analysis tool • Establishing Data Analytics Platform for Cybersecurity - pull in IPS logs, inventory information, firewall logs • Establishing PCN Inventory using discovery tools for IT components • Implemented Firewalls between PCNs and business networks • Implemented Intrusion Prevention Systems on PCNs • Looking to implement Security Information and Event Management (SIEM) on many PCNs which would feed central

		SIEM
	Federal and state incentives available to accelerate investment in and adoption of resilient energy delivery systems	• ESTCP (e.g., Binary Analysis of Firmware) - LBNL
Mid-Term Goals	Collaborative environments, mechanisms, and resources available for connecting security and operations researchers, vendors, and asset owners	• ICS-CERT (DHS) • Vulnerability Assessment Team • ONG-ISAC provides for affiliated membership for third parties and vendors. • Looking to establish Predictive Analytics capability using Hadoop Data Analytics Platform. • Resilience models will be used to improve incident detection/mitigation. • Working towards PCN Cybersecurity workstream in all business plans. The business still owns the PCNs. Would need to continue to plan for security enhancements. This should become a fixed workstream in planning.
	Federally funded partnerships and organizations focused on energy sector cybersecurity become self-sustaining	

U.S. DEPARTMENT OF ENERGY

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology and Engineering Solutions of Sandia LLC, a wholly owned subsidiary of Honeywell International Inc. for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

Sandia National Laboratories

Long-Term Goals	Private sector investment surpasses Federal investment in developing cybersecurity solutions for energy delivery systems	
	Mature, proactive processes to rapidly share threat, vulnerabilities, and mitigation strategies are implemented throughout the energy sector	• DHS • DOD • ONG-ISAC - Oil & Natural Gas Information Sharing & Analysis Center • OGCSN - Oil & Gas Cybersecurity Network • OGBC - Oil & Gas Benchmarking Consortium • API-ITSS - API IT Security Subcommittee • E ISAC - Energy ISAC (Run by NERC) •
Overall Goal	Collaboration between industry, academia, and government maintains cybersecurity advances	• FoxGuard (Pen testing/Vulnerability monitoring) • Partner with government agencies through API ITSS and ONG ISAC. (See Near Term Gap - ONG ISAC) • DHS: Assistant Secretary for Cybersecurity and Communications, the National Cybersecurity and

		Communications Integration Center (NCCIC), US-CERT and ICS-CERT • Oil and Natural Gas Sector Coordinating Council (ONG SCC) and Energy Government Coordinating Council (GCC), especially coordinating with the DHS Assistant Secretary for Infrastructure Protection (IP) and DOE Assistant Secretary for the Office of Electricity and Energy Reliability • FBI National Cyber Investigative Joint Task Force (NCIJTF) • Office of the Director of National Intelligence (ODNI) Trade Association Partners Group • US Coast Guard Office of Port & Facilities Compliance • Vendors should be included in the long-term partnerships to improve security. • In an effort to establish appropriate cooperation and joint efforts, appropriate regulatory framework

		should be established. This would allow for the appropriate cooperation and joint efforts to minimize risks across all PCN environments. Have to share enough information to resolve the problems and minimize risk overall. Must ensure that everyone is brought up to a certain baseline - requires a lot of cooperation and info sharing. May be doing things that in another context could be considered anti-trust.

4. IAB Roadmap Gaps

The IAB similarly identified the existing gaaps within the two strategic areas covered in this report: “Develop and Implement New Protective Measures to Reduce Risk” and “Sustain Security Improvements”. The first strategic area includes new technologies to harden energy delivery systems and make them more resilient to cyber incident while not degrading operational services. The second strategic area focuses on collaboration amongst national laboratories, academia, vendors, and asset owners to ensure that new technologies do not compromise the security of the overall energy delivery system. The following tables describe the areas where the roadmap can be revised to include the enumerated gaps.

4.1 Develop and Implement New Protective Measures to Reduce Risk

	Milestones	Roadmap Gaps
Near-Term Goals	Capabilities to evaluate the robustness and survivability of new	• Looking to develop in-house resilience models for

	platforms, systems, networks, architectures, policies, and other system changes commercially available	cybersecurity drills. Challenge: There is no automated inventory system for OT components to establish visual models of the OT technology. • Third party solutions that are manufactured "overnight" and making it proprietary. Tofino, NERC CIP, not rated to work in SCADA networks (medium, low voltage) - not tested in those environments - A major safety concern. Need certification process for energy world. • A lot of inverters are failing. Inverter mismatch with protocols. Batteries rated at 1 mW but only operates below 1 mW. 2-3 labs that certify PEO office is needed.
Mid-Term Goals	Scalable Access Control for all energy delivery system devices available	• Two factor authentication is a goal. Would like to use Identity Service Provider and SAML Federation for third party authentication. Looking into various secure mechanisms

		for remote access. Some of the Process Automation vendors have begun implementing this capability on their product roadmaps, but it is not ubiquitous. At Layer 3 in the Purdue model, it is becoming more prevalent. • Cost to deploy access control at every site is expensive. Currently, process is to pull ID cards authorization and feed into cyber system. A possible solution is to build a queue within Microsoft to limit access to specific device (one-time sign-on).
	Next-generation, interoperable, and upgradeable solutions for secure serial and routable communications between devices at all levels of energy delivery system networks implemented	• Many PCNs are in remote locations with access to minimal bandwidth. In these cases, the infrastructure must be built. There is a large legacy infrastructure with little or no encryption capabilities. It is difficult to retrofit encryption onto point-to-point or point-to-multi-point microwave

		links. These technologies are dependent on lifecycle for modification. • There is growing awareness of Cloud providers and cloud offerings. Adoption of these cloud services is a challenge. There is some hesitancy in adoption due to culture of in-house monitoring and control.
Long-Term Goals	Self-configuring energy delivery system network architectures widely available	• Do not have self-configuring infrastructure components. • Proprietary solutions are in wide usage
	Capabilities that enable security solutions to continue operation during a cyber attack available as upgrades and built-in to new security solutions	• Would like to be able to use results from cyber resilience models for real-time cyber defense. For example, automated turning on/off of specific components of PCN. However, the capability does not exist yet. • The current state of forensics for control systems is lacking. Additional tools that respect the real-time constraints of control systems are needed.

		- Forensics capabilities to isolate specific location of anomaly (secure enclaves)
	Next-generation, interoperable, and upgradeable solutions for secure wireless communications between devices at all levels of energy delivery system networks implemented	- SDN is a young technology and most SDN offerings are proprietary with limited vendor interoperability. - Look at zigbee protocol using strong encryption keys
Overall Goal	Next-generation energy delivery system architectures provide "defense in depth" and employ components that are interoperable, and able to continue operating in a degraded condition during a cyber incident	- No defense in depth process - checklist married against requirements/regulations. - Automate process of protecting new interfaces that need to be connected to or replaced and tie back to NIST requirements which should be tied to an action. Positive direction matrix that specifies go/no-go decisions.

4.2 Sustain Security Improvements

	Milestones	Roadmap Gaps
Near-Term Goals	Cyber threats, vulnerability, mitigation strategies, and incidents timely shared among appropriate sector stakeholders	- Cyber Physical Security - ONG-ISAC still in early maturity stages. Communications via email. The Automated

		Threat Feed working group has been established to finalize decisions on what platform to use (Soltra or other) for data feeds. The goal is to have the capability/technology in place before the API Conference in November of 2016. This will also include a STIX/TAXII feed from DHS for TLP Amber alerts, once a CRADA is established with DHS. • Need automated inventory tools for OT components of PCN. Inventory tracking is a manual process. • Threat intelligence feeds must be consolidated/packaged and provided to the PCNs workgroups. PCN visibility into threats is challenge. Must develop a rating system for threat intelligence feeds that is applicable to PCNs.
	Federal and state incentives available to accelerate investment in and adoption of resilient energy delivery systems	
Mid-Term Goals	Collaborative	• ONG-ISAC has

	environments, mechanisms, and resources available for connecting security and operations researchers, vendors, and asset owners	applied for a CRADA with DHS, which will allow the (bidirectional) exchange of information with DHS and DHS's National Cybersecurity and Communications Integration Center (NCCIC). This should be in place by end of August, 2016. Quarterly, ONG-ISAC executives meet with DHS and DOE at the Energy Government Coordinating Council (GCC) and Oil and Natural Gas (ONG) Sector Coordinating Council (SCC) meeting. At this meeting, information is exchanged about cyber threats to the ONG sector.
	Federally funded partnerships and organizations focused on energy sector cybersecurity become self-sustaining	
Long-Term Goals	Private sector investment surpasses Federal investment in developing cybersecurity solutions for energy delivery systems	• Agencies bring funding without knowledge. Control of acquisition and program management and contracting. • Differences between

		IT and OT need to be communicated so that cyber security personnel and power engineers can speak the same language.
	Mature, proactive processes to rapidly share threat, vulnerabilities, and mitigation strategies are implemented throughout the energy sector	• Several Critical Infrastructure Industry companies have challenges to incentivize vendors to make hardware and software cybersecurity improvements a standard feature of PCN products.
Overall Goal	Collaboration between industry, academia, and government maintains cybersecurity advances	

5. IAB 2017 Responses

The IAB working group has been in ongoing discussions since June, 2016. The IAB provided valuable updates and feedback to the roadmap with recommendations for areas of future research that the industry is currently not addressing. The gaps identified as part of the 2016 summary are included in Section 4. Our communications with the IAB have been ongoing through 2017 to continue to identify any new research gaps since the 2016 survey. The results received here are in response to the "Strategies for Achieving Energy Delivery Systems in Cybersecurity Milestones Assessment" report from September, 2016. The following questions and responses were sent and received from the working group:

1. What new opportunities for R&D have you observed over the last year that you believe are suitable for the CEDS program to address (areas that industry is not currently addressing)?

   Hardware parts lifetimes are decreasing and are causing several redesigns, particularly when applied towards ICS environments. Improving the supply chains and lifetimes of parts is an area of research that needs to be addressed.

2. What new technologies do you see becoming more prevalent in OT environments in the future (Cloud, IoT, mobile, SDN …)?
   Software Defined Networking (SDN), cloud technologies such as Software as a Service (SaaS) and Network Operating Services (NOC) services.

3. Do you have any examples to monitor system health within OT environments?
   Supervisory Control And Data Acquisition (SCADA), physical contact systems, logging and alerting via syslog, Security Information and security Event Management (SIEM) systems, Software Defined Networking through flow monitoring, and the power system itself.

4. What level of autonomy would you like to see in OT environments?
   While autonomous monitoring has benefits, the collection of log information needs to be integrated into an enterprise level view to allow analysts to connect all the dots from beginning of the attack to the potential end. Separate monitoring of IT and OT environments is a seam that can exploited by attackers. This position is re-enforced on page 34 under “Managing Incidents” by encouraging “SIEM” integration into an EMS of the updated roadmap document. PNNL has an effort going on down this path where the sponsor/project managers are continuously being encourage to not burden the operator with more information about potential cyber/physical attacks. Just make sure the operator knows who to call – great recommendations from 4.2. Application focused automation would be nice so that the end user knows what application they want and the tech can make that application work using the best-known methods followed by locking down that application.

5. What are the biggest security needs in OT environments where there currently is no solution?
   Forensics and asset management are the biggest needs. Tools are needed to provide information regarding system level and network level events to better understand the state of the system in the present and in the past.

6. Has any progress been made in sharing threats within the Energy or Oil & Natural Gas sectors? Are there any specific tools that support sharing of this information that are being used?
   Some ONG are utilizing the Threat Connect portal, in addition to the DNG-ISAC (different from the ONG-ISAC), to share information in real time. This is part of a DHS grant to the Interstate Natural Gas Association of America (INGAA)

for 2017. Extension of the grant has been requested for 2018. Manually sharing is also, of course, an option.

7. Have any specific tools been developed to automatically inventory the systems in operational environments that you have worked with, and if so can you share information more easily?
None that the IAB is aware of.

8. Are there any new publically available data sets that your team has found useful in developing and testing new cybersecurity protections?
None, testing is currently performed using a laboratory environment to simulate an OT environment.

There were also updates from our IAB that were received regarding the “Strategies for Achieving Energy Delivery Systems in Cybersecurity Milestones Assessment” report which are shown below:

SUSTAIN SECURITY IMPROVEMENTS

5.1 Cyber threats, vulnerability, mitigation strategies, and incidents timely shared among appropriate sector stakeholders

- ***2016_Evidence of Progress:***
  - E-ISAC (consistently cited as a good source of information)
  - ONG-ISAC (Oil & Natural Gas Information Sharing & Analysis Center)
- ***2016_Recommendations:***
  - ONG-ISAC is still in early maturity stages. Communications are by email. The Automated Threat Feed working group has been established to finalize decisions on what platform to use for data feeds (Soltra or other). The goal is to have the capability/technology in place before the API Conference in November of 2016. This will also include a STIX/TAXII feed from DHS for TLP Amber alerts, once a CRADA is established with DHS.
- ***2017 ONG-ISAC Update:***
  - ONG-ISAC now leverages an industry leading vendor’s Threat Intelligence Platform (TIP) to aggregate and enrich information from various trusted sources – member companies, governments, and partners such as the E-ISAC. The TIP also supports the automated feed of threat information into member company security tools.

5.3 Collaborative environments, mechanisms, and resources available for connecting security and operations researchers, vendors, and asset owners

- ***2016_Evidence of Progress:***
  - ONG-ISAC provides for affiliated membership for third parties and vendors.
- ***2016_Recommendations:***

    - ONG-ISAC has applied for a CRADA with DHS, which will allow the bi-directional exchange of information with DHS and their National Cybersecurity and Communications Integration Center (NCCIC). This should have been in place by end of August 2016.
    - ONG-ISAC executives meet with DHS and DOE quarterly at the Energy Government Coordinating Council (GCC) and ONG Sector Coordinating Council (SCC) meeting. At this meeting, information is exchanged about cyber threats to the ONG sector.
- ***2017 ONG-ISAC Update:***
    - ONG-ISAC has implemented a CRADA with DHS, which allows for the bi-directional exchange of information with DHS and their National Cybersecurity and Communications Integration Center (NCCIC).
    - ONG-ISAC executives continue to meet with DHS and DOE quarterly at the Energy Government Coordinating Council (GCC) and ONG Sector Coordinating Council (SCC) meeting. At this meeting, information is exchanged about cyber threats to the ONG sector.
    - ONG-ISAC works closely with other ISACs to mutually benefit from the collective knowledge base gained across industries, such as the E-ISAC, FS-ISAC, NC-ISAC, and others as warranted.
    - In 2017, the Department of Energy (DOE) undertook and initiative to strengthen information sharing between their department and the Energy ISACs. ONG-ISAC has joined with other Energy sector ISACs to hold standing tactical and strategic meetings with key points of contact within the intelligence community.

6. Conclusion

The results presented here represent the combined feedback received from the seven established IAB members that SNL has formed. The strategic areas that SNL has focused on in this report include "Develop and Implement New Protective Measures to Reduce Risk" and "Sustain Security Improvements". Based on the results provided by the SNL IAB, most of the milestones called out in the latest revision of the roadmap have been met as shown in the tables above. The only milestones not addressed come from the "Sustain Security Improvements" strategic area. The two milestones not addressed in that strategic area, based on the IAB feedback, are "Federally funded partnerships and organizations focused on energy sector cybersecurity become self-sustaining" - a mid-term goal, and "Private sector investment surpasses Federal investment in developing cybersecurity solutions for energy delivery systems" – a long-term goal. Notable gaps mentioned include improving existing forensic capabilities, automating vulnerability assessment tools, automated inventory tools, addressing legal aspects of new technologies, and ensuring that education and training is included as milestones across the board in both strategic focus areas of SNL. SNL will continue to seek additional IAB members and will remain in contact with the existing IAB. Much of the feedback received was in alignment with the results received from the previous year, for example the need for enhanced forensic capabilities. New areas were also identified such as the need for autonomous systems and application as well as publicly available datasets to help evaluate new cyber security protections.

U.S. DEPARTMENT OF ENERGY

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology and Engineering Solutions of Sandia LLC, a wholly owned subsidiary of Honeywell International Inc. for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

Sandia National Laboratories